U.S. HOUSE OF REPRESENTATIVES HOMELAND SECURITY COMMITTEE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

HEARING – MARCH 17, 2010

AN ASSESSMENT OF CHECKPOINT SECURITY: ARE OUR AIRPORTS KEEPING PASSENGERS SAFE?

WRITTEN TESTIMONY OF COL. (RET) ERIC R. POTTS, INTERIM DIRECTOR - HOUSTON AIRPORT SYSTEM

Good afternoon, Madam Chairwoman and Members of the Committee. Thank you for inviting me to testify today. The Houston Airport System is the fourth-largest multi-airport system in the nation and the sixth-largest in the world. Our flagship airport - George Bush Intercontinental or "IAH" - is one of the country's largest gateways for both domestic and international passengers. It is the nation's eighth-largest passenger airport, and the world's 16th-largest. In 2009 our airports in Houston served approximately 48 million passengers, and projections show some 80 million passengers by 2020. We generate some 151,000 regional jobs and contribute over $24 billion to the local economy. Houston is also a DHS designated tier-1 urban area security initiative city. According to a 2007 regional threat and vulnerability assessment conducted by *Digital Sandbox, Inc.,* IAH is the highest at-risk asset in the entire Southeast Texas area. Given that the Houston metropolitan area has the nation's fourth-largest population and is home to essential elements of our energy supply and refining capacity, effective passenger screening at our airports is one of our top priorities.

Over the course of the past eight (8) years many improvements have been made to the aviation security environment. We work closely with our federal counterparts in the Department of Homeland Security (DHS), and it's a partnership we value greatly. For example, in Houston we have recently partnered with the Transportation Security Administration (TSA) to implement Explosive Detection System (EDS) baggage screening solutions in both major airports (IAH and William P. Hobby Airport (HOU)). Additionally, the Houston Airport System (HAS) and the TSA are actively working together on the Airport Surveillance Program, a project which provides funding for enhancements to the airports' existing Closed Circuit Television (CCTV) and related recording systems, and the TSA is preparing to implement full body scanner equipment at both IAH and HOU.

But while aviation security has improved significantly since 9/11/2001, the threat is an evolving one and much remains to be done. In the past year alone there have been numerous plots to destroy U.S. aviation assets. On an international level, the attempted bombing of a U.S. airliner on Christmas day reminds us that the aviation sector remains vulnerable to exploitation and attack, and within the Texas region, an airport in Dallas was initially assessed as a terrorist target by a self-radicalized extremist who had overstayed his visa.

Airports face special challenges in ensuring airport security. While the federal government plays a key role in airport security matters, federal law imposes principal responsibility on local airport

operators (under 49 CFR §§ 1540 and 1542) for securing the National Aeronautical Domain (NAD) within their particular region. As such, the Houston Airport System has identified many impediments that still exist regarding aviation security – impediments that could be minimized by the procurement of certain security technologies and the institution of certain federal initiatives relative to: 1) intelligence sharing, 2) risk assessment/critical infrastructure protection, and 3) field-based aviation security compliance technology.

There are four key points I want to share with you today, and they all have to do with essential needs that airports such as ours in Houston face. They are the need for:

- Improved, timely intelligence sharing and acquisition of appropriate secure communications equipment to facilitate this;
- Development by DHS of a standardized computer-based risk assessment methodology targeted at threats facing airports;
- Field-based devices for use by local airport security personnel that enable real-time, proactive use of current threat data; and
- Funding to cover the associated costs of these measures and of deployment of TSA's Advanced Imaging Technology units.

Allow me to begin by identifying the single most critical issue for airport operators and their local security directors: the lack of timely and consistent dissemination of national threat intelligence information. This remains a constant frustration – one that even predates the tragedy of 9/11. On the state and local level, intelligence sharing has seen some improvement, but obstacles remain. As the Committee well understands, the primary objective of intelligence sharing in the aviation security industry is to allow for a proactive approach in driving the security posture and program that is implemented at the ground level. However, airport security directors – i.e., the force with the most available security assets at an airport - generally do not receive the information from federal sources that they deem necessary or on a timely basis, even though airports such as HAS employ personnel cleared to the appropriate federal level; at IAH we have more than 200 security personnel, for example.

As a result, airports often are able only to serve as a reactive force as opposed to the preferred proactive security model that we seek to field on a daily basis. The lack of adequate intelligence sharing renders airport security operators in the position of primarily conducting random baseline security measures. But if we received timely and accurate intelligence information we could adjust the airports' security posture to better counter current and evolving threats. Equally, understanding the potential efficacy of various threat streams would enable airport security authorities to proactively devise and employ appropriate countermeasures. The lack of timely and adequate information thus severely limits the proactive role that airport security directors can play, and overall reduces the efficacy of the available resources. This is a major gap in the system and it needs to be closed, and now.

The absence of appropriate secure technology is a major impediment to the sharing of this information, and we understand the challenges that our federal counterparts face in this regard. Unfortunately, comprehending threat, risk and vulnerability – and thus being able to act on that

information - has been greatly restricted due to technology and communication gaps caused by the bureaucracy involved in funding and obtaining the equipment needed to receive classified information. To correct this, certain technology must be made immediately available to the local airport security directors. This includes Secure Terminal Equipment (STE) telephones, a Secure Fax, and connections to the Homeland Secure Data Network (HSDN) and Secret Internet Protocol Router Network (SIPRNet). For example, for nearly four months now in Houston, HAS' Intelligence coordinator, who possesses a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance, has been working with DHS to procure the equipment needed to transact secure communications, but no DHS entity has been willing to provide the sponsorship needed for these acquisitions. While in this case both federal and local intelligence partners have the desire to work collaboratively in the exchange of intelligence information, the systems do not appear to exist that would ensure the prompt and efficient acquisition of the necessary technology at the local level. This requires immediate attention.

The lack of intelligence sharing is further exacerbated by the fact that there is no current federal standard in the utilization of a particular risk assessment methodology across the air domain. While some U.S. airports may have incorporated a risk management program, there has been no standard risk assessment methodology prescribed by DHS. What is needed is a national, intelligence-led, risk-based security doctrine that seeks to target and mitigate vulnerabilities in a proactive and recurring fashion. We believe that DHS should adopt a standard risk assessment methodology for use across the NAD in order to facilitate a fair, equitable and consistent comparison of commercial aviation facilities across the United States. The utility of this security construct is two-fold: 1) it would increase the overall security posture of the national aviation system, and 2) it would enable DHS to allocate scarce funding resources more fairly, consistently and efficiently in addressing deficiencies from one airport facility to another. The integration of effective intelligence technologies and the identification of a particular risk assessment methodology would ultimately provide a more robust means by which to identify and implement appropriate countermeasures in the field, a duty which again is the primary responsibility of the local airport security operator.

To close the loop and bring the benefits of good, timely intelligence information and uniform risk assessments into the field, we also need the prompt implementation of new technology. Therefore, we believe that an additional critical element of a well constructed aviation security program would be the implementation of a standardized national aviation security compliance technology. For example, we would support the uniform implementation of a field-based hardware device loaded with software for data tracking/compliance to capture and data mine relevant security information throughout the aviation threat arena. The field-based reporting system we would support should be capable of capturing instant raw data by security area, category, and department. This raw data could then be used to generate predictive trend analysis and, if tied to a national database, could provide valuable real-time information that could also be analyzed and formed into risk assessment and compliance verification product at the national level. The compliance component of this software would ensure that standard, baseline security protocols mandated by TSA are being met, as well as any other unique local response protocols developed as a result of this intelligence-led, risk-based process.

We are encouraged by the TSA's recent announcement of its plan to install Advanced Imaging Technology (AIT) at security checkpoints to replace current walk-though metal detection devices. This technology has the potential to enhance security and deserves further consideration. The airport industry has always been supportive of TSA's evaluation and installation of new technology to enhance security at the checkpoint and efficiency for the passenger. Unlike walk-through metal detectors, AIT can detect prohibited items that have little or no metallic content. AIT will also allow passengers with surgical implants to avoid the invasive physical pat down inspections that come with walk-through metal detectors. TSA has now deployed the units to more than 19 airports, and is slated to deploy units at several more airports throughout this calendar year. Airports have encouraged TSA to pursue enhancements to checkpoint technology that will increase effectiveness, efficiency and passenger throughput while continuing to provide passengers the option of alternate screening methods, and we see this development as very positive.

However, several concerns remain that require immediate attention. First, many airports have severe limitations on the space requirements needed to install AIT units. Of the airports that responded to a recent survey conducted by Airports Council International – North America (the nation's primary airport trade association), about half reported having limited checkpoint space. In order to accommodate AIT, some airports will lose concession space. This will mean a loss of non-aeronautical revenue during a time when airports are already experiencing extremely tight budgets and traffic declines due to the economy. For others, it will mean a complete reconfiguration of their checkpoint areas or reinforcing their terminal floors in order to support the weight of the units; this also is very expensive. Where will the funding come from for these changes? Many airports already face critical financial challenges, and these will be exacerbated by these additional security requirements. Airports are already severely limited by law in how they can fund their operations, and often face severe opposition when they attempt to increase user fees to accommodate the growing needs of our air transportation system. It is critical that Congress and DHS fully understand and provide for the significant costs associated with additional security requirements; this is not an issue that can be ignored. We need Congress and the DHS/TSA to work with airports to provide funding for the airport modifications necessary for installation of AIT units at airport checkpoints.

In addition to terminal modifications, we are concerned about the throughput time that may be required to process passengers through AIT units as opposed to the time it takes to process them through walk-through metal detectors. TSA has stated that they can process a passenger in 15 seconds; some airports that already have the units at their checkpoints have said that in reality it can take as long as 45 seconds to process one passenger. Airports will continue to work with TSA locally to ensure that passenger queue time remains as efficient as possible, but ultimately airports have no control over the actual processing and utilization of TSA's equipment. Congress needs to provide the direction to DHS/TSA to ensure that these challenges are addressed speedily.

In response to these concerns raised by airports at a recent meeting, Secretary Napolitano asked TSA to create a working group comprised of airport and TSA representatives to develop a coordinated plan for AIT deployment that considers passenger throughput and the costs associated with facility modifications. Although TSA, at the first working group meeting, confirmed that it plans to deploy the

first 500 AIT units only to airports that have available checkpoint space and do not need facility modifications, the issue of checkpoint space and modifications will continue to be challenging for other airports, particularly small airports; this issue requires ongoing attention. Given the lack of available funding necessary for facility modifications at checkpoint locations where space is limited, we hope that the working group process will result in a cooperatively developed technology deployment plan that identifies airport checkpoint locations where AIT can be readily deployed. We do ask however, that TSA provide funding, where necessary, for any terminal modifications or enhancements that may be required in order to properly install AIT units at airport checkpoints across the nation. Congress needs to ensure that the security of our airports does not become an unfunded mandate left for our local communities.

In conclusion, allow me to thank you for the opportunity to testify before the Committee today. In terms of priorities I would like to conclude by asking the Committee to focus on intelligence sharing matters first, the identification of a particular risk assessment methodology second, and the technology based compliance program to follow. Finally, please remember that the fragile state of the aviation industry today cannot sustain the financial impact that the implementation of this overall security strategy will require; the burdens fall primarily on our nation's airports, and considerable additional resources are required. Consequently, I would ask Congress not to impose any further unfunded mandates upon either the commercial aviation industry or the local airport operators that are the cornerstone of the industry.

Madam Chairwoman and Committee Members, thank you for your attention to these important issues. We greatly appreciate your consideration of these needs, which affect all of us and our nation's security as a whole. We stand ready to work with you as necessary to achieve the appropriate solutions.

******